arXiv:0902.3480v2 [math.NT] 28 Jan 2010

# THE ARITHMETIC OF GENUS TWO CURVES WITH (4,4)-SPLIT JACOBIANS

NILS BRUIN AND KEVIN DOERKSEN

Abstract. In this paper we study genus 2 curves whose Jacobians are $(4,4)$-isogenous to a product of elliptic curves. Such Jacobians are called $(4,4)$-split. We consider base fields of characteristic different from 2 and 3, which we do not assume to be algebraically closed. We give a generic model such that any genus 2 curve with geometrically optimally $(4,4)$-split Jacobian can be obtained as a specialization. We also describe the locus of $(4,4)$-split Jacobians in the moduli space of genus 2 curves.

Our main tool is a Galois theoretic characterization of genus 2 curves admitting multiple Richelot isogenies. We also give a general description of Richelot isogenies between Jacobians of genus 2 curves. Previously, only Richelot isogenies with kernels that are pointwise defined over the base field were considered.

## 1. Introduction

Let $k$ be a field and let $C$ be a curve of genus 2 over $k$. Let $J = \mathrm{Jac}(C)$ be its Jacobian. We say that $J$ is *split over* $k$ if $J$ is isogenous over $k$ to a product of elliptic curves $E_1 \times E_2$. The nature of this isogeny can be classified (see Section 2 for definitions):

**Theorem 1** (Kuhn [16, pp. 45–46])**.** *Let $J$ be a Jacobian of a curve $C$ of genus 2 over a field $k$ of characteristic different from 2. Suppose that $J$ is split. Then there are elliptic curves $E_1$, $E_2$ over $k$, and an integer $n > 1$ such that $E_1[n]$ and $E_2[n]$ are isomorphic as group schemes and $J$ is $(n,n)$-isogenous to $E_1 \times E_2$. Furthermore, the curve $C$ admits degree $n$ covers $C \to E_1$ and $C \to E_2$.*

Thus, to describe split Jacobians it is sufficient to describe $(n,n)$-split Jacobians for every $n$. Most results in this direction (see Lange [17], Frey and Kani [9], Kuhn [16] and Shaska [21]) are obtained by the observation that a degree $n$ cover $\psi : C \to E$ of an elliptic curve $E$ by a genus 2 curve $C$ induces a so-called *Frey-Kani cover* $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ completing the commutative diagram

$$\begin{tikzcd} C \arrow[r, "\psi"] \arrow[d, "\pi_C"'] & E \arrow[d, "\pi_E"] \\ \mathbb{P}^1 \arrow[r, "\phi"] & \mathbb{P}^1 \end{tikzcd}$$

One can therefore study the $n$-cover $\psi$ by first considering the map $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$. This approach has been successful in classifying the genus 2 curves with $(n,n)$-split Jacobian over algebraically closed base fields for $n = 3$ ([16, 22, 23]) and $n = 5$ [18]. The cases $n = 2$ and $n = 3$ were also studied classically by Legendre (1832) and Jacobi (1881); see [15, p. 477] or Section 3.

*Date*: January 27, 2010.
1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 14H40.
Research supported by NSERC.

In this paper, we consider the case $n = 4$. We are particularly interested in those $(4,4)$-split Jacobians for which the isogeny does not factor through any elliptic curve isogenies of degree greater than 1. We call those Jacobians *optimally* $(4,4)$-split. In particular, we prove:

**Theorem 2.** *Let $k$ be a field of characteristic distinct from $2, 3$, and let $C$ be a curve of genus $2$ over $k$ whose Jacobian is geometrically optimally $(4,4)$-split. Then there exist $b, c, s \in k$ such that $C$ admits a model (C.1) as given in Appendix C.*

We use the model (C.1) to describe a birational model of the 2-dimensional locus of optimally $(4,4)$-split Jacobians in the moduli-space of curves of genus 2. The *Igusa invariants* $I_2$, $I_4$, $I_6$, and $I_{10}$ (see [11]) of a genus 2 curve $C$ classify the isomorphism class of $C$ over an algebraically closed field. They are homogeneous polynomials of degrees 2, 4, 6, and 10 respectively in the coefficients of the defining polynomial for a model of the genus two curve. This moduli-space is birational to affine 3-space, as given by the *absolute invariants* of a genus two curve [12]:

$$i_1 = 144\frac{I_4}{I_2^2}, \quad i_2 = -1728\frac{(I_2 I_4 - 3I_6)}{I_2^3}, \quad i_3 = 486\frac{I_{10}}{I_2^5}. \tag{1.1}$$

**Theorem 3.** *The absolute invariants $i_1, i_2, i_3$ of a genus $2$ curve with optimally $(4,4)$-split Jacobian satisfy an equation $\mathcal{L}_4$, of weighted degree $90$, where $i_1, i_2, i_3$ are given weights $2, 3, 5$ respectively.*

The equation $\mathcal{L}_4$ is too large to reproduce on paper: it consists of 4574 monomials with coefficients having up to 138 digits. We have therefore made a copy available electronically (see [6]). The surface described by $\mathcal{L}_4$ is the *Humbert surface* of discriminant 16 (see [13]).

*Remark* 4. In Appendix A we use Theorem 3 to verify a classic result by O. Bolza (see [1]). We find that one of his equations has a sign error and that our family is birational to his corrected family.

The paper is laid out in the following way. In Section 3, we review some well-known results about genus two curves with $(2,2)$-split Jacobians. In Section 4, we review $(2,2)$-isogenies on Jacobians of curves of genus two. The results in both of these sections will be used extensively throughout the rest of the paper.

*Remark* 5. In Proposition 11, we determine the appropriate twist of the codomain of a Richelot isogeny. Previous literature only considered the case where the kernel is pointwise defined over the base field (see [7, 10, 25]).

Section 5 outlines our strategy for constructing a genus two curve which has a $(4,4)$-split Jacobian. We do not follow the Frey-Kani approach. Instead, we show that the $(4,4)$-isogeny factors through a $(2,2)$-split Jacobian with two $(2,2)$-isogenies with trivially intersecting kernels.

In Section 6 we study Jacobians of genus 2 curves equipped with two $(2,2)$-isogenies:

**Theorem 6.** *Let $k$ be a field of characteristic disctinct from $2$. The Jacobian of a genus $2$ curve*

$$C : Y^2 = f(X)$$

*has two $(2,2)$ isogenies over $k$ if and only if the Galois group of $f(X)$ is contained in $C_2 \times V_4 \subset S_6$ or $\tilde{S}_3 = \langle (1,3,5)(2,4,6), (12)(36)(45) \rangle \subset S_6$.*

Only the case $\mathrm{Gal}(f) \subset \tilde{S}_3$ can give rise to $(4,4)$-split Jacobians. This information allows us to prove Theorems 2 and 3 in Sections 7 and 8.

*Acknowledgements.* We would like to thank Everett Howe for pointing us to Oskar Bolza's 1887 result [1] described in Appendix A. We are also very thankful for the comments of an anonymous referee. These greatly improved the exposition in this paper.

## 2. $(n,n)$-Split abelian surfaces

Kuhn proves Theorem 1 in the case that the genus two curve $C$ admits a cover $C \to E$, where $E$ is a curve of genus 1. It follows from his argument that $E$ has a rational point.

Note that if $\mathrm{Jac}(C)$ is *split* then there is an isogeny $\mathrm{Jac}(C) \to E_1 \times E_2$. Consequently, we have a non-constant morphism $\mathrm{Jac}(C) \to E_1$. We can map $C \to \mathrm{Jac}(C)$ via $P \mapsto [2P] - \kappa$, where $\kappa \in \mathrm{Pic}^2(C/k)$ is the canonical class. It is straightforward to check that the composition $C \to \mathrm{Jac}(C) \to E_1$ must be non-constant as well, so indeed $C$ is a cover of an elliptic curve $E_1$, although this cover is almost certainly not of minimal degree.

Kuhn also shows that if the two covers $\psi_1 : C \to E_1$ and $\psi_2 : C \to E_2$ do not factor through any other genus 1 covers, then we obtain an $(n,n)$*-isogeny*:

$$0 \to \Delta_n \to E_1 \times E_2 \xrightarrow{\psi_1^* + \psi_2^*} \mathrm{Jac}(C) \to 0,$$

where $\Delta_n = \ker(\psi_1^* + \psi_2^*)$ is isomorphic to both $E_1[n]$ and $E_2[n]$ as finite group schemes. There is an isomorphism $\lambda_n : E_1 \to E_2$ such that

$$\Delta_n = \{(P, \lambda_n(P)) : P \in E_1[n]\}$$

The group schemes $E_1[n]$, $E_2[n]$ and $\mathrm{Jac}(C)[n]$ come equipped with a *Weil-pairing.* This is an alternating, non-degenerate bilinear pairing

$$(\ .\ ,\ .\ )_{E_1} : E_1[n] \times E_1[n] \to \mu_n,$$

where $\mu_n$ is the group scheme of $n$-th roots of unity. The group scheme $(E_1 \times E_2)[n] \simeq E_1[n] \times E_2[n]$ naturally has a pairing as well, by taking the product of the pairings on $E_1[n]$ and $E_2[n]$.

The statement that $\psi_1^* + \psi_2^*$ is an $(n,n)$-isogeny amounts to the fact that the kernel $\Delta_n$ is a *maximal isotropic subgroup* (see for instance [19, Proposition 16.8]). This means that the pairing on $(E_1 \times E_2)[n]$ restricts to the trivial pairing on $\Delta_n$, and that $\Delta_n$ is maximal with that property. For any $P, Q \in E_1[n]$ we have

$$1 = ((P, \lambda_n(P)), (Q, \lambda_n(Q)))_{(E_1 \times E_2)[n]} = (P, Q)_{E_1[n]} \cdot (\lambda_n(P), \lambda_n(Q))_{E_2[n]}.$$

Therefore, $\lambda_n$ is an *anti-isometry* with respect to the Weil-pairing.

Conversely, we see that we can specify any $(n,n)$-split abelian surface by giving two elliptic curves $E_1, E_2$, together with an anti-isometry $\lambda_n : E_1[n] \to E_2[n]$ with respect to the Weil-pairing (see [9]). Over the algebraic closure of $k$, the resulting abelian surface $E_1 \times E_2/\Delta_n$ is principally polarized, and hence, it is either the Jacobian of a genus two curve, the Weil-restriction of an elliptic curve with respect to a quadratic extension, or a direct product of two elliptic curves. In this article, we will describe what happens for $n = 4$.

## 3. (2, 2)-Split Jacobians

This is a brief outline characterizing genus 2 curves with (2, 2)-split Jacobians. See Gaudry and Schost's 2001 paper [10] or Chapter 14 of Cassels and Flynn [7] for a more detailed analysis.

**Theorem 7** (Cassels and Flynn [7, p. 155])**.** *Let $C_2$ be a genus 2 curve with a $(2,2)$ split Jacobian over a field $k$ of odd characteristic and let $\phi : \mathrm{Jac}(C_2) \to E_1 \times E_2$ be the $(2,2)$ isogeny. Then the curves $C_2, E_1, E_2$ admit models:*

$$\begin{aligned} C_2 &: Y^2 = c_3X^6 + c_2X^4 + c_1X^2 + c_0 \\ E_1 &: V^2 = c_3U^3 + c_2U_2 + c_1U + c_0 \\ E_2 &: Z^2 = c_0W^3 + c_1W^2 + c_2W + c_3. \end{aligned}$$

*Furthermore, we have the covers*

$$\begin{array}{cccccc} \psi_1 : & C_2 & \to & E_1 & \\ & (X,Y) & \mapsto & (X^2, Y) & = (U,V) \end{array} \qquad \begin{array}{cccccc} \psi_2 : & C_2 & \to & E_2 & \\ & (X,Y) & \mapsto & (1/X^2, Y/X^3) & = (W,Z) \end{array}$$

Conversely, given two elliptic curves $E_1, E_2$ with $\lambda_2 : E_1[2] \xrightarrow{\sim} E_2[2]$, one can make an abelian variety $A$ that is $(2,2)$-isogenous to $E_1 \times E_2$. If a model of $E_1$ is given by $V^2 = c_3U^3 + c_2U_2 + c_1U + c_0$, then $E_1$ is a double cover of the $U$-line, ramified above the roots of $c_3U^3 + c_2U_2 + c_1U + c_0$ and $\infty$. We express $E_2$ as a double cover of the $U$-line as well, such that for each of the three order 2 points $T \in E_1[2]$, we have $U(T) = U(\lambda_2(T))$. We write $0_1 \in E_1$ and $0_2 \in E_2$ for the identity points. We have $U(0_1) = \infty$. If $U(0_2) \neq \infty$, then we can ensure by an affine coordinate transformation that $U(0_2) = 0$. This places us in the situation of Theorem 7 and hence we have that $A = \mathrm{Jac}(C_2)$.

If $U(0_2) = \infty$, then we have that $E_1$ and $E_2$ are geometrically isomorphic and that $\lambda_2$ is induced by a geometric isomorphism $E_1 \xrightarrow{\sim} E_2$. Note that even if the $j$-invariant of $E_1$ is 0 or 1728, the only automorphisms that preserve full level 2 structure are $[1], [-1]$. Hence, if $E_1, E_2$ are geometrically isomorphic with isometric 2-torsion, then $E_2$ must be a (possibly trivial) quadratic twist of $E_1$.

If $E_1 \simeq E_2$, we simply recover the $(2,2)$-isogeny $E_1 \times E_1 \to E_1 \times E_1$ given by $(P,Q) \mapsto (P+Q, P-Q)$. In general, we obtain a $(2,2)$-isogeny to an abelian surface that is a *Weil Restriction*, $\Re_{k(\sqrt{d})/k}(E_1)$, which is an abelian surface such that for any $k$-algebra $A$, we have $\Re_{k(\sqrt{d})/k}(E_1)(A) \simeq E_1(A \otimes_k k(\sqrt{d}))$ (see [2, § 7.6]).

**Lemma 8.** *Let $E$ be an elliptic curve over a field $k$ of odd characteristic. Let $d \in k^*$ be non-square and let $E^{(d)}$ be the quadratic twist of $E$ by $d$. Then there is a $(2,2)$-isogeny*

$$\Re_{k(\sqrt{d})/k}(E) \to E \times E^{(d)}.$$

*Proof.* We write $\sigma$ for the generator of $\mathrm{Gal}(k(\sqrt{d})/k)$. One can construct $\Re_{k(\sqrt{d})/k}(E)$ by appropriately twisting the action of $\sigma$ on $E \times E$. In particular, one obtains

$$\Re_{k(\sqrt{d})/k}(E)(A) = \{(P, {}^\sigma P) : P \in E(A \otimes_k k(\sqrt{d}))\}.$$

The isogeny arises from

$$\begin{array}{ccc} \Re_{k(\sqrt{d})/k}(E) & \to & E \times E^{(d)} \\ (P, {}^\sigma P) & \mapsto & (P + {}^\sigma P, P - {}^\sigma P) \end{array}$$

In order to check that this isogeny is indeed a $(2,2)$-isogeny, we note that this property is preserved under base extension. Over $k(\sqrt{d})$, we have:

$$\begin{tikzcd}
E\times E: \arrow[d] \arrow[dd, bend right, "{[2]}"'] \arrow[dr] & (P,Q) \arrow[dr, mapsto] & \\
\Re_{k(\sqrt{d})/k}(E) \arrow[r, leftrightarrow, "\sim"] \arrow[d] & E\times E: \arrow[dl] & (P+Q,P-Q) \arrow[dl, mapsto] \\
E\times E: & (2P,2Q) &
\end{tikzcd}$$

Hence, we see that the kernel of $E\times E \to \Re_{k(\sqrt{d})/k}(E)$ is also the kernel of a $(2,2)$-isogeny defined over $k(\sqrt{d})$, and hence $E\times E \to \Re_{k(\sqrt{d})/k}(E)$ is a $(2,2)$-isogeny itself. □

*Remark* 9. If $E$ has a square discriminant and has non-zero $j$-invariant, then there are isometries $E[2]\to E[2]$ over $k$ that do not come from an automorphism $E\to E$. These lead to $(2,2)$-isogenies between $E\times E$ and the Jacobian of a curve of genus 2. This construction arises in our analysis of $(4,4)$-split surfaces; see (7.12) and Remark 18.

## 4. (2,2)-Isogenies on Jacobians

In this section, we introduce $(2,2)$-isogenies between Jacobians of genus 2 curves, also known as *Richelot isogenies*. See also [25, Chapter 8], [7, Chapter 9] [4], or [8, Section 4]. Let $k$ be a field of odd characteristic, let $\overline{k}$ be an algebraic closure of $k$ and let $C$ be a curve of genus 2 over $k$. Then $C$ admits a model of the form

$$C : Y^2 = f(X) = f_6X^6 + f_5X^5 + \cdots + f_1X + f_0, \tag{4.1}$$

where $f(X)\in k[X]$ is a square-free polynomial of degree 5 or 6. If $k$ has at least 6 elements, then we can assume that $f_6 \neq 0$. There are some curves over $k = \mathbb{F}_3, \mathbb{F}_5$ that escape our analysis but their base extensions to $\mathbb{F}_9$ and $\mathbb{F}_{25}$ do fall within our scope. Note that $(f_6Y)^2 = f_6^2 f(X)$ is also a model of $C$ over $k$, so it is not a restriction to insist that the leading coefficient is a cube. We assume that $f_6 = q_2^3$ for some $q_2 \in k$.

Let $w_1,\dots,w_6$ be the roots of $f(X)$ in $\overline{k}$. The Weierstrass points of $C$ are exactly $T_i = (w_i, 0)$. The non-zero two-torsion points in $\operatorname{Pic}^0(C/\overline{k})$ are exactly the divisor classes $T_{\{i,j\}} = [T_i - T_j] = [T_j - T_i]$, and the Weil-pairing is given by

$$(T_{\{i,j\}}, T_{\{k,l\}})_2 = (-1)^{\#\{i,j,k,l\}}.$$

Let $J = \operatorname{Jac}(C)$. The maximal isotropic subgroups of $J[2]$ are exactly of the form

$$\{0, T_{\{i_1,i_2\}}, T_{\{i_3,i_4\}}, T_{\{i_5,i_6\}}\},$$

where the indices are given by a partition $\{\{i_1,i_2\},\{i_3,i_4\},\{i_5,i_6\}\}$ of $\{1,\dots,6\}$ into three disjoint pairs. For ease of notation, we assume that $(i_1,\dots,i_6) = (1,\dots,6)$. This data corresponds to specifying a factorization

$$F_j(X) = q_2X^2 + q_{1,j}X + q_{0,j} = q_2(X - w_{2j-1})(X - w_{2j})$$

such that

$$f(X) = F_1(X)F_2(X)F_3(X).$$

We say that $\{F_1(X), F_2(X), F_3(X)\} \subset \overline{k}[X]$ is a *quadratic splitting* of $f$ and if $\{F_1(X), F_2(X), F_3(X)\}$ is stable under $\mathrm{Gal}(\overline{k}/k)$ then we say that it is a quadratic splitting of $f$ *over* $k$. Note that the $F_i(X)$ do not have to be individually defined over $k$.

Let $\phi : \mathrm{Jac}(C) \to B$ be an isogeny with kernel $\{0, T_{\{1,2\}}, T_{\{3,4\}}, T_{\{5,6\}}\}$. This kernel is defined over $k$ if and only if the corresponding quadratic splitting is.

We know that $B$ is either the Jacobian of a curve of genus 2 or the product of two elliptic curves over $\overline{k}$. The latter happens precisely when

$$\delta = \det \begin{pmatrix} q_{0,1} & q_{1,1} & q_2 \\ q_{0,2} & q_{1,2} & q_2 \\ q_{0,3} & q_{1,3} & q_2 \end{pmatrix} = 0 \tag{4.2}$$

(see [25, page 117] or [7, page 89]). We say $\delta$ is the *determinant* of the quadratic splitting. If $\delta = 0$ then we say the quadratic splitting $\{F_1(X), F_2(X), F_3(X)\}$ is *singular*. Otherwise, $B$ is the Jacobian of a genus 2 curve and we say $\{F_1(X), F_2(X), F_3(X)\}$ is *nonsingular*. We will determine $B$.

Suppose $\{F_1(X), F_2(X), F_3(X)\}$ is nonsingular. Then for $(i, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2)$ we define

$$G_i(X) = \delta^{-1} \det \begin{pmatrix} \frac{d}{dX} F_j(X) & \frac{d}{dX} F_k(X) \\ F_j(X) & F_k(X) \end{pmatrix}$$

where $\delta$ is defined as in (4.2). It is straightforward to check that $\{G_1(X), G_2(X), G_3(X)\} \subset \overline{k}[X]$ is again stable under $\mathrm{Gal}(\overline{k}/k)$. For $d \in k^*$, we consider the curve

$$\tilde{C}_d : d\tilde{Y}^2 = g(\tilde{X}) = G_1(\tilde{X}) G_2(\tilde{X}) G_3(\tilde{X}). \tag{4.3}$$

**Lemma 10.** *The polynomial $g$ is squarefree of degree 5 or 6.*

*Proof.* This follows by direct computation; see [25, Page 122]. □

It follows that $\tilde{C}_1$ is a curve of genus 2 and that $B = \mathrm{Jac}(\tilde{C}_1)$ over $\overline{k}$. In fact, for an appropriate value of $d$, we have that $B = \mathrm{Jac}(\tilde{C}_d)$ over $k$. In order to see this, we consider a curve $\Gamma \subset C \times \tilde{C}_d$, defined over $\overline{k}$ by

$$\Gamma_d : \begin{cases} F_1(X)G_1(\tilde{X}) + F_2(X)G_2(\tilde{X}) & = & 0 \\ F_1(X)G_1(\tilde{X})(X - \tilde{X}) & = & \sqrt{d}\,\tilde{Y}Y \\ F_2(X)G_2(\tilde{X})(X - \tilde{X}) & = & -\sqrt{d}\,\tilde{Y}Y \end{cases}$$

If $F_1, F_2, F_3 \in k[X]$ and $d = 1$, then $\Gamma_d$ is defined over $k$. In that case, the curve describes a $(2,2)$-correspondence, called a *Richelot correspondence*, between $C$ and $\tilde{C} = \tilde{C}_1$, which gives rise to an isogeny of the desired type (see [25, Theorem 8.4.11] or [4, Section 3.1]).

If $F_1$ and $F_2$ are quadratic conjugate, say over an extension $k(\sqrt{d})$, then $F_3$ is necessarily defined over $k$. Then the set of defining equations for $\Gamma_d$ is $\mathrm{Gal}(\overline{k}/k)$-stable, and hence $\Gamma_d$ is defined over $k$. Since over $\overline{k}$, the curves $\tilde{C}_d$ and $\Gamma_d$ are isomorphic to $\tilde{C}_1$ and $\Gamma_1$, it follows from the above discussion that $\Gamma_d$ describes a correspondence giving rise to an isogeny $\mathrm{Jac}(C) \to \mathrm{Jac}(\tilde{C}_d)$ of the desired type.

If $\mathrm{Gal}(\overline{k}/k)$ acts transitively on $\{F_1, F_2, F_3\}$, then the field of definition of $Q(X) = F_1(X)$ is a cubic extension $A$ of $k$. The $F_i$ are the images of $Q(X)$ under the three possible $k$-algebra homomorphisms $A \to \overline{k}$. In fact, the other cases can be described in the same manner if we allow $A$ to be a cubic étale algebra rather than a field. Let $h(T) \in k[T]$ be a square-free cubic such that the $\mathrm{Gal}(\overline{k}/k)$ action on its roots in $\overline{k}$ is the same as on $\{F_1, F_2, F_3\}$. Then

$A = k[T]/(h(T))$ and the $F_j(X)$ are the images of some $Q(X) \in A[X]$ under the three possible non-constant $k$-algebra homomorphisms $A \to \overline{k}$. We can write

$$f(X) = \mathrm{Norm}_{A[X]/k[X]}(Q(X)).$$

We see that specifying a quadratic splitting of $f(X)$ over $k$ corresponds exactly to writing $f(X)$ as a norm of a quadratic polynomial over a cubic algebra over $k$. This description allows us to concisely state which $d$ one should choose in (4.3):

**Proposition 11.** *Let $h(T) \in k[T]$ be a square-free cubic polynomial, let $A = k[T]/(h(T))$ and $Q(X) \in A[X]$ a quadratic polynomial. Suppose that*

$$C : Y^2 = f(X) = \mathrm{Norm}_{A[X]/k[X]}(Q(X))$$

*is a curve of genus 2. Let $d = \mathrm{disc}(h(T))$ and let*

$$\tilde{C} : d\tilde{Y}^2 = G(\tilde{X})$$

*be defined as in (4.3). If $\tilde{C}$ is a curve of genus 2 then $\mathrm{Jac}(C)$ and $\mathrm{Jac}(\tilde{C})$ are $(2,2)$-isogenous over $k$, with kernel as described above.*

*Proof.* We can prove this by considering a generic model over $k$. Let $K = k(h_0, h_1, h_2, q_{i,j})$ with $i, j \in \{0, 1, 2\}$, let $A = K[T]/(T^3 + h_2 T^2 + h_1 T + h_0)$ and let $Q \in A[X]$ be defined by

$$Q = \sum_{i,j=0}^{2} q_{i,j} T^j X^i.$$

We now consider the curve $C : Y^2 = f(X) = \mathrm{Norm}_{A[X]/k[X]}(Q(X))$ over $K$. Let $L$ be the splitting field of $h(T) = T^3 + h_2 T^2 + h_1 T + h_0$. Then $L$ is a degree 6 extension of $K$. Furthermore, $A$ is a cubic subfield and $L = A(\sqrt{d})$ where $d = \mathrm{disc}(h(T))$. Over $L$, we have $f(X) = F_1(X)F_2(X)F_3(X)$, where, say $F_3(X) \in A[X]$ and $F_1(X)$ and $F_2(X)$ are quadratic conjugate over $A$. Using the discussion above, we see that $\phi : \mathrm{Jac}(C) \to \mathrm{Jac}(\tilde{C}_d)$ over $A$. Note that $C_d$ is already defined over $K$. Thus over $K$, we must have that the codomain is isomorphic to some twist of $\mathrm{Jac}(\tilde{C}_d)$ that is trivial when base extended to $A$. For genus 2, this implies that it is the Jacobian of some twist of $C_d$. However, $\tilde{C}_d$ is a generic genus 2 curve and hence only has quadratic twists. Since any element $d' \in K^*$ that becomes a square in $A^*$ is already a square in $K^*$, it follows that the codomain is indeed $\mathrm{Jac}(\tilde{C}_d)$.

The proposition now follows by observing that any curve $C$ over $k$ of the required type can be obtained by specializing $q_{i,j}, h_0, h_1, h_2$. □

Note that this result does not rule out the existence of $(2,2)$-isogenies between Jacobians that are not presented as the type given. We only prove that the codomain *can* be represented as $\mathrm{Jac}(\tilde{C})$. Abelian varieties that can be expressed as Jacobians in multiple ways are extremely special, though.

## 5. $(4,4)$-split Jacobians

Let $C_4$ be a genus two curve with $(4,4)$-split Jacobian $J_4$. By Theorem 1, we have an isogeny $\Psi_4 : E_1 \times E_2 \to J_4$ with kernel $\Delta_4 \subset E_1[4] \times E_2[4]$. Furthermore, we have a Weil-pairing anti-isometry $\lambda_4 : E_1[4] \to E_2[4]$ such that $\Delta_4$ is the image of the map $P \mapsto (P, \lambda_4(P))$.

Since $E_i[2] \subset E_i[4]$, we also have $\lambda_2 = \lambda_4|_{E_1[2]} : E_1[2] \to E_2[2]$. Hence, we can construct an abelian surface $A$, with an isogeny $\Psi_2 : E_1 \times E_2 \to A$ where $\ker(\Psi_2) = \Delta_2 = \Delta_4 \cap (E_1 \times E_2)[2]$. It follows that $\Delta_2$ is maximal isotropic, so $\Psi_2$ is a $(2,2)$-isogeny.

The isogeny $\Psi_4$ factors through $A$ as

$$\begin{tikzcd} E_1 \times E_2 \arrow[r, "\Psi_2"] \arrow[rr, bend right, "\Psi_4"'] & A \arrow[r, "\Phi"] & J_4 \end{tikzcd} .$$

Similarly, the multiplication $[2] : E_1 \times E_2 \to E_1 \times E_2$ factors through $A$ as well, giving

$$\begin{tikzcd} E_1 \times E_2 \arrow[rr, "\Psi_4"] \arrow[dr, "\Psi_2"] \arrow[dd, "{[2]}"'] & & J_4 \\ & A \arrow[ur, "\Phi"'] \arrow[dl, "\Psi_2^*"] & \\ E_1 \times E_2 & & \end{tikzcd}$$

**Lemma 12.** *The isogeny $\Phi : A \to J_4$ is a $(2,2)$-isogeny. Furthermore,* $\ker(\Phi) \cap \ker(\Psi_2^*) = \{0\}$.

*Proof.* The kernel of $\Psi_2$ is isomorphic to $E_1[2]\,(\cong E_2[2])$. Similarly, the kernel of $\Psi_4$ is isomorphic to $E_1[4]$ and $\ker(\Psi_2) \subset \ker(\Psi_4)$. Let $H$ denote the image of $\ker(\Psi_4)$ under $\Psi_2$. Then $H \cong \ker(\Psi_4) / \ker(\Psi_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Furthermore, the Weil-pairing on $H$ is trivial because it is induced by the Weil-pairing on $\Delta_4$.

In order to see that $\ker(\Phi) \cap \ker(\Psi_2^*) = \{0\}$, note that $\Psi_2$ is injective on $E_1[2] \times \{0\}$ and maps it onto $\ker(\Psi_2^*)$, because $\Psi_2^* \circ \Psi_2 = [2]$. Since $\Phi \circ \Psi_2$ is injective on $E_1[4] \times \{0\}$, it follows that $\Phi$ is also injective on $\Psi_2(E_1[2] \times \{0\}) = \ker(\Psi_2^*)$. This shows that $\ker(\Phi) \cap \ker(\Psi_2^*) = \{0\}$. $\square$

The diagram also shows that the analysis from Section 3 applies to $A$. If $E_1$ and $E_2$ are not geometrically isomorphic, then $A = \mathrm{Jac}(C_2)$ is a $(2,2)$-split Jacobian of a genus 2 curve. Otherwise, $A$ may be isomorphic to $\Re_{k(\sqrt{d})/k}(E_1)$ or $E_1 \times E_1$. The latter case implies that $J_4$ is already $(2,2)$-split, so that case is not interesting for describing optimally $(4,4)$-split Jacobians.

In the next sections, we will concentrate on the general case $A = \mathrm{Jac}(C_2)$. Remark 17 shows that the case where $A$ is a Weil restriction occurs for a large part as a limit. From the discussion above, we see that $\mathrm{Jac}(C_2)$ is $(2,2)$-split via $\Psi_2^*$ and has a second $(2,2)$-isogeny $\Phi$ with $\ker(\Phi) \cap \ker(\Psi_2^*) = \{0\}$. In Section 7 we will classify such $C_2$.

## 6. 2-level structure on curves of genus 2

Let $k$ be a field of characteristic different from 2. Any curve of genus 2 can be obtained by specializing $(f_0, \ldots, f_6)$ in the curve

$$C_{\underline{f}} : Y^2 = f(X) = f_6 X^6 + f_5 X^5 + \cdots + f_0$$

over $k(\underline{f}) = k(f_6, f_5, \ldots, f_0)$. Similarly, any curve of genus 2 with all of its Weierstrass points labeled can be obtained by specializing $(w_1, \ldots, w_6, f_6)$ in the curve

$$C_{\underline{w}} : Y^2 = f_6(X - w_1) \cdots (X - w_6)$$

over $k(\underline{w}) = k(f_6, w_1, \ldots, w_6)$. Of course, one can just forget a labelling to obtain a curve $C_{\underline{f}}$ from $C_{\underline{w}}$. This allows us to express $k(\underline{w})$ as a finite extension of $k(\underline{f})$ via

$$\begin{aligned} f_5 &= -f_6(w_1 + \cdots + w_6) \\ f_4 &= f_6(w_1w_2 + w_1w_3 + \cdots + w_5w_6) \\ &\vdots \\ f_0 &= f_6 w_1 \cdots w_6 \end{aligned}$$

In fact, $k(\underline{w})$ is a splitting-field of $f(X)$ over $k(\underline{f})$ and $\mathrm{Gal}(k(\underline{w})/k(\underline{f})) = S_6$.

From the fact that a two-torsion point $T \in \mathrm{Jac}(C)[2](\overline{k})$ can be represented uniquely as $T_{\{i,j\}} = [(w_i, 0) - (w_j, 0)]$, it follows that a full labelling of the Weierstrass points on a curve of genus 2 induces a full labelling of the two-torsion of the Jacobian of $C$ and vice versa. The cognoscenti will recognize that this reflects the isomorphism $\mathrm{Sp}_4(\mathbb{F}_2) \simeq S_6$.

It is instructive to see how this connects to the corresponding moduli spaces. We can view $k(\underline{w})$ and $k(\underline{f})$ as the function fields of $\mathrm{PGL}_2(k)$-covers of the corresponding moduli-spaces in the following way: The fractional linear transformations on the $X$-line below $C$ induce a $\mathrm{PGL}_2(k)$-action on $k(\underline{f})$ and $k(\underline{w})$. If we divide out by this action, we obtain a relation with the function fields of the coarse moduli spaces $\mathcal{M}_2$ of curves of genus 2 and $\mathcal{M}_2(2)$ of curves of genus 2 with full level 2-structure on their Jacobians.

$$\begin{tikzcd}
k(\underline{w}) \arrow[dr, "./\mathrm{PGL}_2(k)"] \arrow[dd, "./S_6"'] & \\
& k(\mathcal{M}_2(2)) \arrow[dd, "./\mathrm{Sp}_4(\mathbb{F}_2)"] \\
k(\underline{f}) \arrow[dr, "./\mathrm{PGL}_2(k)"'] & \\
& k(\mathcal{M}_2)
\end{tikzcd}$$

*Proof of Theorem 6.* As outlined in Section 4, specifying a $(2,2)$-isogeny on $\mathrm{Jac}(C)$ corresponds to a partitioning of the roots of $f(x)$ into $\{\{w_1, w_2\}, \{w_3, w_4\}, \{w_5, w_6\}\}$. This corresponds to some partial level 2 structure and specifies some intermediate function field $k(\underline{f}) \subset K_1 \subset k(\underline{w})$. Via Galois theory, $K_1$ corresponds to the conjugacy class of some subgroup of $S_6$, fixing a partitioning of the type $\{\{1,2\},\{3,4\},\{5,6\}\}$. Indeed, the stabilizer $H_1$ of $\{\{1,2\},\{3,4\},\{5,6\}\}$ is of order 48 and is isomorphic to $(C_2)^3 \rtimes S_3$, see Figure 1. The group $H_1$ has 3 orbits, of lengths 1, 6 and 8 respectively, on the set of partitionings of $\{1, \ldots, 6\}$ into 3 disjoint unordered pairs: 6 partitionings that share one tuple with $\{\{1,2\},\{3,4\},\{5,6\}\}$ and 8 that do not. This gives two subgroup conjugacy classes that fix two partitionings, as given in Figure 1. Each actually fixes three partitionings. In the given presentation we have that $\tilde{S}_3$ fixes

$$\big\{\{1,2\},\{3,4\},\{5,6\}\big\},\ \big\{\{1,4\},\{2,5\},\{3,6\}\big\},\ \big\{\{1,6\},\{2,3\},\{4,5\}\big\} \tag{6.1}$$

and that $C_2 \times V_4$ fixes

$$\big\{\{1,2\},\{3,4\},\{5,6\}\big\},\ \big\{\{1,2\},\{3,5\},\{4,6\}\big\},\ \big\{\{1,2\},\{3,6\},\{4,5\}\big\}. \tag{6.2}$$

$\square$

$$\begin{tikzcd}[column sep=small]
& k(\underline{w}) \arrow[dl, dash] \arrow[dr, dash] & & & \langle(1)\rangle \arrow[dl, dash] \arrow[dr, dash] & \\
K_2 \arrow[dr, dash] & & K_3 \arrow[dl, dash] & \tilde{S}_3 \arrow[dr, dash] & & C_2 \times V_4 \arrow[dl, dash] \\
& K_1 \arrow[d, dash] & & & (C_2)^3 \rtimes S_3 \arrow[d, dash] & \\
& k(\underline{f}) & & & S_6 &
\end{tikzcd}$$

$$\begin{aligned}
(C_2)^3 \rtimes S_3 &= \langle (12), (34), (56), (13)(24), (15)(26) \rangle \\
\tilde{S}_3 &= \langle (135)(246), (12)(36)(45) \rangle \\
C_2 \times V_4 &= \langle (12), (34)(56), (35)(46) \rangle
\end{aligned}$$

FIGURE 1. Galois groups associated to intermediate 2-level structure

**Lemma 13.** *Let $C_4$ be a curve of genus 2 over $k$ and suppose that $\mathrm{Jac}(C_4)$ is geometrically optimally $(4,4)$-split. Then $\mathrm{Jac}(C_4)$ is $(2,2)$-isogenous to $\mathrm{Jac}(C_2)$ where $C_2$ is a curve of genus 2 admitting a model of the form*

$$C_2 : Y^2 = g(X) = f(X^2) = c_3X^6 + c_2X^4 + c_1X^2 + c_0,$$

*such that $g(X)$ and $f(X)$ have the same splitting field, $K$, and $\mathrm{Gal}(K/k)$ is isomorphic to a subgroup of a conjugate of $\tilde{S}_3$.*

*Proof.* By the discussion in Section 5, we have a $(2,2)$-split abelian surface $A$, together with a $(2,2)$-isogeny $\Phi : A \to \mathrm{Jac}(C_4)$. Since we are assuming that $\mathrm{Jac}(C_4)$ is geometrically optimally split, we must have $A = \mathrm{Jac}(C_2)$ for some genus 2 curve $C_2$. By Theorem 7, the curve $C_2$ admits a model of the form

$$C_2 : Y^2 = g(X) = f(X^2) = c_3X^6 + c_2X^4 + c_1X^2 + c_0,$$

where $V^2 = f(U)$ is a model of an elliptic curve which is a degree 2 subcover of $C_2$.

Let $L$ denote the splitting field of $g$ and let $K$ denote the splitting field of $f$. Then $K$ is an extension of $k$, and either $L$ is a degree two extension of $K$ or $L = K$. By the discussion immediately prior to Lemma 13, we must have $\mathrm{Gal}(L/k) \leq \tilde{S}_3$ or $\mathrm{Gal}(L/k) \leq C_2 \times V_4$.

Suppose $\mathrm{Gal}(L/k) \not\leq \tilde{S}_3$. The three viable kernels for the $(2,2)$-isogenies are given by the partitionings in equation (6.2). In particular, writing $T_{\{i,j\}}$ for the two-torsion point $[(w_i, 0) - (w_j, 0)]$ then there is a labeling of the roots of $f(x)$ such that the possible kernels are:

$$\left\{0, T_{\{1,2\}}, T_{\{3,4\}}, T_{\{5,6\}}\right\}, \quad \left\{0, T_{\{1,2\}}, T_{\{3,5\}}, T_{\{4,6\}}\right\}, \quad \left\{0, T_{\{1,2\}}, T_{\{3,6\}}, T_{\{4,5\}}\right\} \tag{6.3}$$

Notice that the pairwise intersection of these kernels is in all cases $\left\{0, T_{\{1,2\}}\right\} \neq \{0\}$, contradicting Lemma 12. Therefore $\mathrm{Gal}(L/k) \leq \tilde{S}_3$.

The three kernels of the $(2,2)$-isogenies that are fixed by $\tilde{S}_3$ are given by the partitionings in (6.1). A simple verification shows that $\tilde{S}_3$ acts faithfully on each of these kernels. In particular, if $\{0, T_1, T_2, T_3\}$ is the kernel of the singular $(2,2)$-isogeny $\mathrm{Jac}(C_2) \to E_1 \times E_2$,

then $\tilde{S}_3$ has the canonical $S_3$-action on $\{T_1, T_2, T_3\}$. Thus, $\tilde{S}_3$ has the usual $S_3$ action on the roots of $f$. It follows $f$ and $g$ have the same splitting field. $\square$

## 7. Bielliptic genus 2 curves with $S_3$ as a Galois group

In this section, we give something close to a universal model for the genus 2 curve $C_2$ from Lemma 13. Since the corresponding moduli space of genus 2 curves is not a fine moduli space (the space $\mathcal{M}_2(2)$ is not even fine), a universal curve does not exist. However, by allowing extra parameters, we can still give a family that covers all possible $C_2$ by specialization, similar to how any elliptic curve can be obtained by specializing a general Weierstrass model $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$.

Let $k$ be a field of characteristic distinct from 2 or 3. Let $C_2$ be a genus 2 curve over $k$ with a $(2,2)$-split Jacobian and let $E_1$ be a degree 2 subcover of $C_2$. Then $E_1$ has a model $V^2 = f(U) = U^3 + bU + c$ and $\mathrm{Gal}(f)$, the Galois group of $f$, is a subgroup of $S_3$. In order to produce the family, we concentrate on the most general case $\mathrm{Gal}(f) = S_3$. We will argue later that other cases are also parametrized.

Genus 2 curves that are 2-covers of $E_1$ have models of the form $Y^2 = g(X)$, where:

$$g(X) = f\left(\frac{X^2}{d} + a\right)$$

with $a, d \in k$ (see [5, Section 5] or [7, Chapter 14]). The Jacobian of the genus 2 curve is $(2,2)$-isogenous to $E_1 \times E_2$, where $E_2$ has a model:

$$W^2 = d(U-a)f(U)$$

Working in the extension $k[U]/(f(U)) = k[r]$, the polynomials $f$ and $g$ factor as

$$\begin{aligned} f(U) &= (U-r)\left(U^2 + rU + \left(r^2+b\right)\right) \\ g(X) &= \frac{1}{d^3}\left(X^2 + ad - rd\right)\left(X^4 + (dr+2ad)X^2 + d^2r^2 + ad^2r + a^2d^2 + bd^2\right) \end{aligned} \tag{7.1}$$

Let $h(X)$ denote the (monic) quartic factor of $g$ in (7.1):

$$h(X) = X^4 + (dr+2ad)X^2 + d^2\left(r^2 + ar + a^2 + b\right). \tag{7.2}$$

We want $g$ to split over the same field as $f$. In order for this to occur, $h$ must be reducible over $k(r)$. Otherwise $h$ would be irreducible and we would require a degree 4 extension over $k(r)$ to split $h$. The following lemma from Kappe and Warren's paper [14] gives us testable conditions on $h$:

**Lemma 14** (Kappe and Warren)**.** *Let $h(x) = x^4 + bx^2 + d$ be a polynomial over a field $k$ of characteristic $\neq 2$ and let $\pm\alpha$, $\pm\beta$ be its roots. Then the following conditions are equivalent:*

*(1) $h(x)$ is irreducible over $k$;*
*(2) The following are not squares in $k$:*
  *(i) $b^2 - 4d$,*
  *(ii) $-b + 2\sqrt{d}$, and*
  *(iii) $-b - 2\sqrt{d}$.*

We can use Lemma 14 to determine the conditions on $a$ and $d$ such that $h$ factors as a product of two quadratics over $k(r)$. In our case, the polynomial $h$ will be reducible over $k(r)$ if one of the following is true:

(i) $(dr+2ad)^2 - 4d^2\left(r^2 + ar + a^2 + b\right)$ is a square in $k(r)$, or

(ii) $-(dr+2ad)+2d\sqrt{r^2+ar+a^2+b}$ is a square in $k(r)$, or
(iii) $-(dr+2ad)-2d\sqrt{r^2+ar+a^2+b}$ is a square in $k(r)$.

Taking the conditions one at a time, in case (i), after simplification, we require $-3r^2-4b$ to be a square. Observe that this is the discriminant of $x^2+rx+(r^2+b)$ and hence occurs exactly when our original polynomial $f(x)$ splits over $k(r)$. This contradicts $\mathrm{Gal}(f)=S_3$, so we ignore this possibility for now.

In the remaining two cases, we require $r^2+ar+a^2+b$ to be a square in $k(r)$. Let $t\in k(r)$ such that $r^2+ar+a^2+b=t^2$. Since $k(r)$ is a cubic extension of $k$, we can set $t=t_2r^2+t_1r+t_0$. It follows that

$$\begin{aligned} r^2+ar+a^2+b &= \left(t_2r^2+t_1r+t_0\right)^2 \\ &= t_2^2r^4+2t_1t_2r^3+\left(t_1^2+2t_0t_2\right)r^2+2t_0t_1r+t_0^2 \\ &= \left(t_1^2+2t_0t_2-bt_2^2\right)r^2+\left(2t_0t_1-2bt_1t_2-ct_2^2\right)r+\left(t_0^2-2ct_1t_2\right). \end{aligned}$$

Equating coefficients, we obtain the system of three equations:

$$\begin{aligned} t_1^2+2t_0t_2-bt_2^2-1&=0 \\ -a+2t_0t_1-2bt_1t_2-ct_2^2&=0 \\ a^2+b-t_0^2+2ct_1t_2&=0 \end{aligned} \tag{7.3}$$

We obtain an affine variety $X$ in $\mathbb{A}^4$ with parameters $b$ and $c$. Working in Magma [3], we find that $X$ has two components, interchanged by $(a,t_0,t_1,t_2)\mapsto(a,-t_0,-t_1,-t_2)$. Each component is a genus 0 curve in $\mathbb{A}^4$. Using Magma, we can parametrize this curve. Let $s\in k$ denote a parameter; then:

$$\begin{aligned} a &= \frac{s^4-2bs^2-8cs+b^2}{4\left(s^3+bs+c\right)} \\ t_0 &= \frac{-s^4-6bs^2-4cs-b^2}{4\left(s^3+bs+c\right)} \\ t_1 &= \frac{-s^3+bs+2c}{2\left(s^3+bs+c\right)} \\ t_2 &= \frac{-3s^2-b}{2\left(s^3+bs+c\right)}. \end{aligned} \tag{7.4}$$

For any $s\in k$, this parametrization gives a value for $a$ such that $r^2+ar+a^2+b$ is a square in $k(r)$. Using the parametrization, we can express the square root of $r^2+ar+a^2+b$ as:

$$\frac{-3s^2-b}{2\left(s^3+bs+c\right)}r^2+\frac{-s^3+bs+2c}{2\left(s^3+bs+c\right)}r+\frac{-s^4-6bs^2-4cs-b^2}{4\left(s^3+bs+c\right)}.$$

This allows us to evaluate the expressions in (ii) and (iii):

In case (ii), using our parametrization for $a$, we find $-(dr+2ad)+2d\sqrt{r^2+ar+a^2+b}$ becomes

$$\left(-\frac{1}{4\left(s^3+bs+c\right)}\right)\cdot d\cdot F_1$$

where $F_1 = (6s^3 + 2bs)\, r^2 - (6s^3 + 2bs)\, r - (3s^4 + 2bs^2 - 12cs + 3b^2)$. This is a square in $k(r)$ if and only if

$$d = -\left(s^3 + bs + c\right) \cdot \square \tag{7.5}$$

where $\square$ represents any square.

Using this parametrization for $a$ and $d$, we find that $g(X) = f(X^2/d + a)$ has the same splitting field as $f$. The Galois group of $g$ is indeed isomorphic to $S_3$. In fact, its representation in $S_6$ is $S_3'' = \langle (123)(456), (23)(56) \rangle$ which is not conjugate to $\tilde{S}_3$ from Section 6. Therefore, by Lemma 13, the Jacobian of the genus 2 curve $C : Y^2 = g(X)$ does not have two $(2,2)$-isogenies with trivially intersecting kernels.

In case (iii), using the paramatrization for $a$, we find $-(dr + 2ad) - 2d\sqrt{r^2 + ar + a^2 + b}$ becomes:

$$\left(-\frac{1}{4\,(s^3 + bs + c)}\right) \cdot d \cdot F_2$$

where $F_2 = (6s^2 + 2b)\, r^2 - (2s^3 + 6bs + 8c)\, r - (s^4 + 10bs^2 - 20cs + b^2)$. This will be a square in $k(r)$ if and only if

$$\begin{aligned} d &= \left(4b^3 + 27c^2\right)\left(s^3 + bs + c\right) \cdot \square \\ &= -D \cdot f(s) \cdot \square \end{aligned} \tag{7.6}$$

where $\square$ represents any square and $D$ is the discriminant of $f$.

Using this parametrization, our hyperelliptic curve $C_2$ is given by $Y^2 = g(X)$ where:

$$\begin{aligned} g = \frac{1}{(4b^3 + 27c^2)^3\,(s^3 + bs + c)^3} X^6 &+ \frac{3\,(s^4 - 2bs^2 - 8cs + b^2)}{4\,(4b^3 + 27c^2)^2\,(s^3 + bs + c)^3} X^4 \\ &+ \frac{P(b,c,s)}{16\,(4b^3 + 27c^2)\,(s^3 + bs + c)^3} X^2 \\ &+ \frac{(s^6 + 5bs^4 + 20cs^3 - 5b^2s^2 - 4bcs - b^3 - 8c^2)^2}{64\,(s^3 + bs + c)^3} \end{aligned} \tag{7.7}$$

and where $P$ is given by

$$P = 3s^8 + 4bs^6 - 48cs^5 + 50b^2s^4 + 128bcs^3 + 4b^3s^2 + 192c^2s^2 - 16b^2cs + 3b^4 + 16bc^2.$$

As desired, we find that $g$ has the same splitting field as $f$ and that $\mathrm{Gal}(g) \simeq \tilde{S}_3$ as found in Section 6. The factorization for $g$ over its splitting field is given in appendix B.

**Lemma 15.** *For any choices $b, c, s \in k$ such that we have a genus 2 curve*

$$C_2 : Y^2 = g(X) \text{ with } g(x) \text{ as in (7.7)}, \tag{7.8}$$

*its Jacobian $\mathrm{Jac}(C_2)$ is $(2,2)$-split and admits a second $(2,2)$-isogeny with trivially intersecting kernel. Conversely, if $C_2$ is a bielliptic genus 2-curve as occurring in Lemma 13 then there exist $b, c, s \in k$ such that (7.8) gives a model.*

*Proof.* The first statement follows from the construction of (7.7).

To show the second part, assume that $\mathrm{Jac}(C_2)$ is $(2,2)$-isogenous to $E_1 \times E_2$. We can choose $b, c$ such that $E_1$ admits a model of the form $E_1 : V^2 = U^3 + bU + c$. The $(2,2)$-isogeny implies that $E_1$ and $E_2$ have isomorphic 2-torsion, so $E_2$ admits a model of the form

$$E_2 : W^2 = d(U - a)(U^3 + bU + c).$$

It remains to show that we can choose $a, d$ as in (7.4) and (7.6).

For any given $b, c$, we can let $s$ vary and get a one-parameter family of bielliptic genus 2 curves with an extra $(2,2)$-isogeny. This means that for any elliptic curve $E_1$, we can construct a 1-parameter family of elliptic curves $E_{2,s}$ such that we have isogenies

$$\begin{tikzcd} E_1 \times E_{2,s} \arrow[r, "\Psi_2"] \arrow[rr, bend right, "\Psi_4"'] & \mathrm{Jac}(C_2) \arrow[r, "\Phi"] & B \end{tikzcd},$$

where $\Psi$ is the second isogeny afforded by $\mathrm{Jac}(C_2)$. One can check that since $\ker \Psi_2^* \cap \ker \Phi = \{0\}$, the map $\Psi_4$ must be a $(4,4)$-isogeny. Hence, there is an anti-isometry $\lambda : E_1[4] \to E_{2,s}[4]$. In particular, this means that $E_{2,s}$ is a family of elliptic curves with constant (meaning independent of $s$) 4-torsion. We write $X^-_{E_1}(4)$ for the twist of the modular curve $X(4)$ that parametrizes elliptic curves with an anti-isometry to $E_1[4]$, which is a fine moduli space. We know that $X(4)$ is a $\mathrm{PSL}_2(\mathbb{Z}/4\mathbb{Z})$-cover of the $j$-line $X(1)$, and hence that $X^-_{E_1}(4) \to X(1)$ is of degree 24.

Our construction expresses the $s$-line as a cover of $X^-_{E_1}(4)$. Straightforward computation shows that $j(E_{2,s})$ is a degree 24-function in $s$ as well. Hence, it follows that $s \mapsto E_{2,s}$ defines a birational map $\mathbb{P}^1_s \to X^-_{E_1}(4)$. This shows that $E_{2,s}$ is a universal curve over $X^-_{E_1}(4)$ and that, outside a locus of codimension at least 1, we can indeed choose $a, d$ as in (7.4) and (7.6). It remains to check that the choices of $s$ for which our construction degenerates, correspond to genuinely degenerate configurations.

Indeed, one can check that $g(X)$ degenerates if $a = a(s) = \infty$ or $a(s)^3 + ba(s) + c = 0$. In all these situations, we have that $E_{2,s}$ is isomorphic to a twist of $E_1$ and that the anti-isometry $E_1[2] \to E_{2,s}[2]$ encoded in our choice of $a$ corresponds to the obvious one. This is exactly the situation in Lemma 8, so in those cases the $(2,2)$-isogenous abelian surface is generally not a Jacobian of a genus 2 curve. □

To find all $(2,2)$-isogenies on $C_2$, we consider all 15 different quadratic splittings over $k[r, R]$. We can then calculate the 15 distinct $(2,2)$-correspondences of $C_2$ by using the 15 distinct quadratic splittings as described in Section 4. We are interested in finding which of these correspondences are defined over the base field.

As expected, we find that one of the quadratic splittings is singular. The singular quadratic splitting is

$$\{q_2(X - w_1)(X - w_2), q_2(X - w_3)(X - w_4), q_2(X - w_5)(X - w_6)\}$$

where $w_i$ are the roots of $g$ over $k[r, R]$ and $q_2^3 = f_6$ is the leading coefficient of $g$ as listed in Appendix B. This singular splitting is due to the $(2,2)$-isogeny $\Psi_2^* : \mathrm{Jac}(C_2) \longrightarrow E_1 \times E_2$. A representation of $E_2$ is given by:

$$E_2 : W^2 = d(U - a)f(U) = -\operatorname{disc}(f) \cdot f(s) \cdot \left(U - \frac{s^4 - 2bs^2 - 8cs + b^2}{4f(s)}\right) \cdot f(U) \tag{7.9}$$

where $a$ is given as in equation (7.4) and $d$ is given as in equation (7.6).

We also find that applying the Richelot correspondence (4.3) to the 14 non-singular quadratic splittings, produces only two $k$-rational sextics, with the remaining twelve defined over $\bar{k}$, but not over $k$. The two quadratic splittings which yield the $k$-rational Richelot

correspondences are

$$\{q_2(X-w_1)(X-w_6), q_2(X-w_2)(X-w_3), q_2(X-w_4)(X-w_5)\} \text{ and} \tag{7.10}$$

$$\{q_2(X-w_1)(X-w_4), q_2(X-w_2)(X-w_5), q_2(X-w_3)(X-w_6)\}. \tag{7.11}$$

Notice that the singular quadratic splitting, together with the two quadratic splittings (7.10) and (7.11) come from the three partitionings that are fixed by $\tilde{S}_3$, given by (6.1).

Let $G_1$ and $G_2$ denote the sextics obtained by applying Richelot's construction (4.3) of $f$ to the quadratic splittings (7.10) and (7.11) respectively. We find that $G_2(X) = G_1(-X)$, and therefore that both models are isomorphic. This is expected, because $E_1 \times E_2$ has an extra automorphism $[1] \times [-1]$. Hence, the existence of one $(4,4)$-isogeny $\Psi_4$ implies the existence of a second $\Psi_4 \circ ([1] \times [-1])$, with the same codomain.

Proposition 11 allows us to select the right twist

$$C_4 : Y^2 = DG_1(X) = F(X) \text{ where } D = \operatorname{disc}(f) = -4b^3 - 27c^2$$

(see Appendix C for $F(X)$, with the extraneous factor $f_6^2$ removed). Looking at the denominators and the discriminant of the sextic given in Appendix C, we find

$$\operatorname{disc}(F) = \frac{2^6\,(s^3+bs+c)^{22}\,(s^6+5bs^4+20cs^3-5b^2s^2-4bcs-b^3-8c^2)}{(4b^3+27c^2)^{14}\,(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2)^{18}}$$

and hence

**Proposition 16.** *The model $C_4$ describes a genus 2 curve unless one of the following holds:*

*(1)* $4b^3 + 27c^2 = 0$,
*(2)* $3bs^4 + 18cs^3 - 6b^2s^2 - 6bcs - b^3 - 9c^2 = 0$,
*(3)* $s^3 + bs + c = 0$, *or*
*(4)* $s^6 + 5bs^4 + 20cs^3 - 5b^2s^2 - 4bcs - b^3 - 8c^2 = 0$.

We can explain each of these degeneracies:

(1) In this case $E_1$ is not an elliptic curve.

(2) Let $\delta$ denote the determinant of the quadratic splitting (7.10). Then

$$N_{k[r,R]/k}(\delta) = \left(4b^3+27c^2\right)^2\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^2,$$

so we see that in this case the $(2,2)$-isogeny $\operatorname{Jac}(C_2) \xrightarrow{\Phi} B$ is given by a singular quadratic splitting. Hence $B$ is indeed not given as a Jacobian of a genus 2 curve.

(3,4) These conditions coincide with $x = s$ corresponding to a 4-torsion point on $E_1$. In these cases we have that $x = a(s)$ corresponds to a 2-torsion point which occur as degenerate cases in Lemma 15 as well.

Hence, in these cases the intermediate abelian surface $A$ occurring in $E_1 \times E_2 \xrightarrow{\Psi_2} A \xrightarrow{\Phi} B$ is not a Jacobian and $E_2$ is isomorphic to a twist of $E_1$. Either the abelian variety $A$ is a Weil-restriction, or $A \simeq E_1 \times E_1$. In the latter case, we see that $B$ is $(2,2)$-split and hence not interesting for our study of optimally $(4,4)$-split Jacobians. As described in Remark 17, we can recover $A = \Re_{k(\sqrt{d})/k}(E_1)$ as a limit $s \to \infty$. This shows that if $E_1[4]$ admits only two anti-isometries $\pm\lambda_4 : E_1[4] \to E_1^{(d)}[4]$ over $k$, then the corresponding $(4,4)$-split abelian variety must be the one arising from this limit.

*Remark* 17. One may wonder how $C_4$ degenerates for the various values of $s$. One case, $s=\infty$, was intentionally left out of Proposition 16. It is the only generically rational point at which the model for $C_4$ as given is degenerate. However, if we consider the isomorphic model $(s^3Y)^2 = F(Xs^2)/s^6$ then we can take $s=\infty$ to obtain the curve

$$C: Y^2 = -64bc\frac{1}{D^3}X^6 + \frac{64}{3}b\frac{1}{D^2}X^5 + 16bc\frac{1}{D^2}X^4 + \frac{224}{27}b\frac{1}{D}X^3 + 4bc\frac{1}{D}X^2 + \frac{4}{3}bX - bc, \tag{7.12}$$

where $D = \operatorname{disc}(f) = -4\,b^3 - 27\,c^2$. The curve $C$ describes a genus 2 curve unless $D=0$ or $b=0$.

It is straightforward to check that $C$ has an extra involution $X \mapsto \frac{D}{4X}$ and hence that $\operatorname{Jac}(C)$ is $(2,2)$-split over $k(\sqrt{D})$. Indeed, if $D$ is not a square, we see that $\operatorname{Jac}(C)$ is $(2,2)$-isogenous to $\Re_{k(\sqrt{D})/k}(E)$. Using Lemma 8, we see that $\operatorname{Jac}(C)$ is $(4,4)$-isogenous to $E\times E^{(D)}$, where $E^{(D)}$ is the quadratic twist of $E$ by $D$.

*Remark* 18. We also see that if $D$ is a square, then $\operatorname{Jac}(C)$ is $(2,2)$-isogenous to $E\times E$, completing Remark 9. The question now arises whether $E\times E$ will in general be optimally $(4,4)$-isogenous to a Jacobian of a genus 2 curve. We can answer this question by using the same construction but with different parameters. By changing the coordinates on $C$ such that the additional involution fixes $0,\infty$ rather than $\pm\sqrt{D}$, we can ensure that $C$ admits a model of the form stated in Theorem 7. If we set

$$E_1 : V_1^2 = U^3 + b\,U + c \text{ and } E_2 : V_2^2 = d(U-a)(U^3 + b\,U + c)$$

then we find for

$$a = \frac{1}{6\,b}(\pm\sqrt{D} - 9c)$$

and an appropriate value for $d$, that $E_1 \simeq E_2$. The question whether this glueing of $E[2]$ with itself is compatible with an auto-anti-isometry of $E[4]$ amounts to checking whether Equation (7.4) can be solved for some $s\in k$. It is straightforward to verify that this need not be the case.

**Corollary 19.** *Let $E$ be an elliptic curve over a field $k$ with* $\operatorname{char}(k)\neq 2$. *Let $D$ be the discriminant of $E$. Then there is an anti-isometric isomorphism $\lambda_4 : E[4] \to E^{(D)}[4]$ with respect to the Weil-pairing.*

*Proof.* If the discriminant $D$ is not a square, then this is clear. Remark 18 completes the case for square $D$. ☐

*Remark* 20. From the construction, it was already clear that (7.9) gives a family of elliptic curves with constant (meaning independent of $s$) 4-torsion. In other words, (7.9) gives the generic point on some twist of the full modular curve $X(4)$. Thanks to Corollary 19, we now see that (7.9) parametrizes the elliptic curves with 4-torsion isometric to $E^{(D)}[4]$ with respect to the Weil pairing. Compare [24].

*Remark* 21. There is a Galois-representation theoretic way of proving Corollary 19. Let $E$ be an elliptic curve over a field $k$ with discriminant $D$ and let $\rho : \operatorname{Gal}(\overline{k}/k) \to \operatorname{Aut}(E[4])$ be the mod 4 Galois representation. We have $\operatorname{Aut}(E[4]) \simeq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. Let $H$ be the subgroup of elements that act via even permutation on the 2-torsion elements. Note that $D$ is also the discriminant of the 2-torsion algebra, so $\rho^{-1}(H) = \operatorname{Gal}(\overline{k}/k(\sqrt{D}))$.

Consider

$$M = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$$

and let $\lambda_M : E[4] \to E[4]$ be the corresponding automorphism. One can check that $\{M, -M\}$ is the unique conjugacy class of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ of size 2 and that the centralizer of $M$ is $H$. It follows that $\lambda_M$ is defined over $k(\sqrt{D})$. Furthermore, since

$$M \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M^T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

we see that $\lambda_M : E[4] \to E[4]$ is an *anti*-isometry.

Now consider the quadratic twist $E^{(D)}$ of $E$. There is an isomorphism $E \to E^{(D)}$ defined over $k(\sqrt{D})$, which when restricted, yields an isometry $\lambda^{(D)} : E[4] \to E^{(D)}[4]$. The composition $\lambda^{(D)} \circ \lambda_M : E[4] \to E^{(D)}[4]$ is an anti-isometry. Furthermore, if $\sigma \in \mathrm{Gal}(\overline{k}/k)$ and $\sigma(\sqrt{D}) = -\sqrt{D}$ then $\sigma(\lambda_M) = -\lambda_M$ and $\sigma(\lambda^{(D)}) = -\lambda^{(D)}$. Hence, $\sigma(\lambda^{(D)} \circ \lambda_M) = \lambda^{(D)} \circ \lambda_M$, so we see that $E[4]$ and $E^{(D)}[4]$ are anti-isometric over $k$.

## 8. Proof of theorems 2 and 3

We can now prove the main theorems given in the introduction of this article.

*Proof of Theorem 2.* Let $C$ be a genus 2 curve whose Jacobian is geometrically optimally $(4,4)$-split. Then by Lemma 13, $\mathrm{Jac}(C)$ is $(2,2)$-isogenous to $\mathrm{Jac}(C_2)$, where $C_2$ is a curve of genus 2, which by Lemma 15, admits a model of the form given in (7.7). The model of the genus 2 curve which is $(2,2)$-isogenous to $C_2$ is given by Theorem 16 and is presented in Appendix C. □

Let $\mathcal{X}$ denote the equation of the surface of genus 2 curves with $(4,4)$-split Jacobians. This surface is the Humbert surface of discriminant 16 and it is irreducible (see [13, Corollary 1.6] and [20]).

We can calculate the Igusa invariants $I_2$, $I_4$, $I_6$, $I_{10}$ of $C_4$. These are given as functions in $b$, $c$, and $s$. Using (1.1), we obtain a system of 3 equations in the absolute invariants $i_1$, $i_2$, and $i_3$ and in $b$, $c$, and $s$. It is too large a system to be able to use Gröbner bases or resultants to eliminate $b$, $c$ and $s$.

We can, however, solve this system modulo $p$ for various large primes $p$. We guessed the degrees and then interpolated the equation mod $p_i$ for 93 consecutive 6-digit primes $p_i$. For each prime, we found a unique solution for the system. We then used rational reconstruction to solve the system mod $N = \prod_{i=1}^{93} p_i$. This yields the equation of a surface $\mathcal{L}_4$ in affine 3-space of the absolute invariants $i_1, i_2, i_3$ of a genus 2 curve. The equation of the surface is too large to reproduce here: $\mathcal{L}_4$ contains 4574 monomials with coefficients having up to 138 digits. We do, however, know that it is irreducible as it was the unique solution found modulo each of the large primes. If the equation were reducible, then there would be multiple solutions corresponding to the factors of $\mathcal{L}_4$.

So far, we have shown $\mathcal{L}_4 \equiv \mathcal{X} \pmod{N}$. In fact, we claim that $\mathcal{L}_4 = \mathcal{X}$. This would be true if we chose a bound $N$ for our rational reconstruction which is greater than twice the max height of the coefficients of $\mathcal{X}$. We had a reasonable expectation that our choice of $N = \prod_{i=1}^{93} p_i \approx 10^{600}$ was large enough as all of the coefficients of $\mathcal{L}_4$ have much smaller size than $\sqrt{N}$.

*Proof of Theorem 3.* To show $\mathcal{L}_4 = \mathcal{X}$, we will show that $\mathcal{L}_4$ has the same zero set as $\mathcal{X}$. We can evaluate distinct points on $\mathcal{X}$ by evaluating equation (C.1) for distinct values of $(b, c, s)$ and calculating the absolute invariants of the curves.

Without loss of generality over an algebraically closed field, we can set $b = 1$ (for a Zariski-open part). From a model of $C_4$, we can find the absolute invariants as rational functions $i_1(b, c, s)$, $i_2(b, c, s)$, and $i_3(b, c, s)$. The expression $\mathcal{L}_4\left(i_1(c, s), i_2(c, s), i_3(c, s)\right) = 0$ gives rise, after clearing denominators, to a polynomial $p(c, s)$ of degrees at most 1800 and 4050 in $c$ and $s$ respectively.

Proving that $\mathcal{L}_4(i_1, i_2, i_3) = 0$ for $(i_1, i_2, i_3) \in V(\mathcal{X})$ amounts to proving that in fact $p(c, s) = 0$. Expanding $p(c, s)$ explicitly is computationally infeasible, so instead, we evaluate $p(c, s)$ over a large number of distinct values for $c$ and $s$. For a fixed value $s = s_0$, if we show that $p(c, s_0) = 0$ at 1801 distinct values for $c$, then $p(c, s_0)$ is the zero polynomial on the line $s = s_0$. If we repeat this process on 4501 distinct lines $s = s_i$ then $p(c, s)$ is in fact the zero polynomial. This calculation was performed in parallel on multiple computers over the course of several weeks. $\square$

## Appendix A. On a classical result by Bolza

An 1887 paper by O. Bolza [1] discusses hyperelliptic integrals which can reduce into elliptic integrals by a fourth degree transformation. In modern terminology, he computes a model of a genus 2 curve with a $(4, 4)$-split Jacobian. In this section we relate his results to ours. The formulas given here are available electronically from [6]. Bolza works over $\mathbb{C}$. He gives a 3-parameter family of curves $y^2 = R(x)$, with parameters $\lambda, \mu, \nu$, with a sign error in the equation (A.3) below. Corrected, Bolza's family is given by:

$$C_{(\lambda,\mu,\nu)} : y^2 = R(x) = \nu' x^6 - 6\lambda\nu' x^5 + 3\left(4\mu\nu' + \lambda\mu'\right)x^4 + 2\left(\lambda\lambda' + 5\nu\nu'\right)x^3 + 3\left(4\mu'\nu + \lambda'\mu\right)x^2 - 6\lambda'\nu x + \nu,$$

where

$$\lambda' = -\frac{1}{3} \cdot \frac{2\lambda^2\nu - \lambda\mu^2 - \mu\nu}{-\nu^2 + 3\lambda\mu\nu - 2\mu^3}, \tag{A.1}$$

$$\mu' = \frac{1}{9} \cdot \frac{\lambda^2\mu + \lambda\nu - 2\mu^2}{-\nu^2 + 3\lambda\mu\nu - 2\mu^3}, \tag{A.2}$$

$$\nu' = -\frac{1}{27} \cdot \frac{2\lambda^3 - 3\lambda\mu + \nu}{-\nu^2 + 3\lambda\mu\nu - 2\mu^3}. \tag{A.3}$$

He also gives the variable substitutions that turn the hyperelliptic integrals into elliptic integrals. In modern language, he gives the degree 4 maps from the curve $C_{(\lambda,\mu,\nu)}$ to two elliptic curves. Since Bolza is only interested in curves over $\mathbb{C}$, he does not care to determine the appropriate twist, but this is easily adjusted. With

$$z_1 = \frac{\lambda x^4 + 4\lambda\nu x + 3\mu\nu}{\lambda x^2 + 2\lambda x + \frac{3\mu\lambda - 2\nu}{2}}, \quad z_2 = \frac{\lambda' + 4\lambda'\nu' x^3 + 3\mu'\nu' x^4}{x^2(\lambda' + 2\lambda' x + \frac{3\mu'\lambda' - 2\nu'}{2}x^2)}$$

we find that $C_{(\lambda,\mu,\nu)}$ covers the two curves

$$E_{1,(\lambda,\mu,\nu)} : w_1^2 = \lambda R_1(z_1) = \lambda(\lambda z_1 - 2\nu)(\nu' z_1^3 - 3(9\lambda^2\nu' - 6\mu\nu' - \lambda\mu')z_1^2 + 12(9\lambda\nu\nu' + 3\mu'\nu + \lambda'\mu)z_1 + 12\nu(3\mu\mu' - \lambda\lambda'))$$

and

$$E_{2,(\lambda,\mu,\nu)} : w_2^2 = \lambda' R_2(z_2) = \lambda'(\lambda' z_2 - 2\nu')(\nu z_2^3 - 3(9\lambda'^2\nu - 6\mu'\nu - \lambda'\mu)z_2^2 + 12(9\lambda'\nu'\nu + 3\mu\nu' + \lambda\mu')z_2 + 12\nu'(3\mu'\mu - \lambda'\lambda)).$$

Checking this is straightforward by verifying that $\lambda R_1(z_1)R(x)$ and $\lambda' R_2(z_2)R(x)$ are squares in $\mathbb{Q}(\lambda,\mu,\nu)(x)$.

In order to find the relation between Bolza's family and the model (C.1), we put $E_{1,(\lambda,\mu,\nu)}$ in short Weierstrass form $V^2 = U^3 + bU + c$, where

$$\begin{aligned} b &= 3(\nu^2 - 3\nu\mu\lambda + 2\mu^3)^2(2\nu^4\mu - 5\nu^4\lambda^2 + 2\nu^3\mu\lambda^3 + 16\nu^3\lambda^5 - \nu^2\mu^4 + \\ &\qquad 10\nu^2\mu^3\lambda^2 - 45\nu^2\mu^2\lambda^4 - 6\nu\mu^5\lambda + 36\nu\mu^4\lambda^3 - 9\mu^6\lambda^2) \\ c &= (\nu^2 - 3\nu\mu\lambda + 2\mu^3)^3(\nu^7 - 3\nu^6\mu\lambda - 10\nu^6\lambda^3 - 10\nu^5\mu^3 + 84\nu^5\mu^2\lambda^2 - 138\nu^5\mu\lambda^4 + 160\nu^5\lambda^6 - \\ &\qquad 30\nu^4\mu^4\lambda + 68\nu^4\mu^3\lambda^3 - 78\nu^4\mu^2\lambda^5 - 288\nu^4\mu\lambda^7 - 2\nu^3\mu^6 + 30\nu^3\mu^5\lambda^2 - \\ &\qquad 189\nu^3\mu^4\lambda^4 + 738\nu^3\mu^3\lambda^6 - 18\nu^2\mu^7\lambda + 198\nu^2\mu^6\lambda^3 - 729\nu^2\mu^5\lambda^5 - \\ &\qquad 54\nu\mu^8\lambda^2 + 324\nu\mu^7\lambda^4 - 54\mu^9\lambda^3). \end{aligned}$$

We compute the linear transformation $U = \frac{t_1 z_2 + t_2}{t_3 z_2 + t_4}$ such that $\lambda' R_2(z_2) = d(U-a)(U^3+bU+c)$, where $d$ is specified up to squares, and find

$$\begin{aligned} a &= \frac{(\nu^2 - 3\nu\mu\lambda + 2\mu^3)(2\nu^3\lambda - 3\nu^2\mu^2 - 4\nu^2\lambda^4 + 2\nu\mu^3\lambda + 6\nu\mu^2\lambda^3 - 3\mu^4\lambda^2)}{\mu\lambda - \nu} \\ d &= 3(\nu - \mu\lambda)(\nu^2 - 3\nu\mu\lambda + 2\mu^3)(\nu^2 - 6\nu\mu\lambda + 4\nu\lambda^3 + 4\mu^3 - 3\mu^2\lambda^2). \end{aligned}$$

From $a = \frac{s^4 - 2bs^2 - 8cs + b^4}{4(s^3 + bs + c)}$ one finds one rational choice:

$$s = \frac{(\nu^2 - 3\nu\mu\lambda + 2\mu^3)(\nu^3\lambda + 3\nu^2\mu^2 - 18\nu^2\mu\lambda^2 + 16\nu^2\lambda^4 + 10\nu\mu^3\lambda - 15\nu\mu^2\lambda^3 + 3\mu^4\lambda^2)}{\nu - \mu\lambda}.$$

This shows that outside $(\nu - \mu\lambda)(\nu^2 - 3\nu\mu\lambda + 2\mu^3) = 0$, Bolza's family covers the family (C.1). The relation turns out to be birational: both $(\lambda : \mu : \nu)$ and $(s : b : c)$ are naturally coordinates on weighted projective space $\mathbb{P}(1,2,3)$. The formulae above express $(b/s^2, c/s^3)$ as functions in $(\mu/\lambda^2, \nu/\lambda^3)$. Via the appropriate resultant computations and polynomial factorizations, we find

$$\begin{aligned} \psi(b,c,s) &= 2b^6 + 36b^5s^2 + 45b^4cs + 72b^4s^4 + 45b^3c^2 + 36b^3cs^3 - 36b^3s^6 + 297b^2c^2s^2 - 378b^2cs^5 \\ &\quad + 54b^2s^8 + 324bc^3s - 81bc^2s^4 + 324bcs^7 + 216c^4 - 324c^3s^3 + 891c^2s^6 - 27cs^9 \\ \frac{\mu}{\lambda^2} &= \frac{(2b^4 - 15b^2cs + 30b^2s^4 + 9bc^2 + 90bcs^3 + 135c^2s^2 - 27cs^5)\psi(b,c,s)}{3(bs + c + s^3)^2(b^2 - 6bs^2 - 12cs - 3s^4)^2(4b^3 + 27c^2)} \\ \frac{\nu}{\lambda^3} &= \frac{-\psi(b,c,s)^2}{(bs + c + s^3)^2(b^2 - 6bs^2 - 12cs - 3s^4)^3(4b^3 + 27c^2)} \end{aligned}$$

This shows that outside some codimension one locus, the two families parametrize the same curves up to twist. Note, however, that the formulas for $a, b, c, d$ are of weighted total degrees $13, 26, 39, 15$ in $(\lambda, \mu, \nu)$. That means that with appropriate scaling, we can adjust the square class of $d$, so the two families really do parametrize essentially the same curves.

## Appendix B. The six roots of the defining polynomial for $C_2$

Let $C_2$ be a genus 2 curve over $k$ which is $(2,2)$-isogenous to a genus 2 curve whose Jacobian is optimally $(4,4)$-split (see Lemma 13). Then $C_2$ is a degree 2 cover of an elliptic curve $E_1$ which admits a model $V^2 = f(U) = U^3 + bU + c$. A model for $C_2$ is given in (7.7).

$$f(U) = (U - r)\left(U^2 + rU + \left(r^2 + b\right)\right)$$

Over $k[r]/\left[U^2 - (-3r^2 - 4b)\right] = k[r, R]$, we have the factorisation

$$f(U) = (U - r)\left(U - \frac{R}{2} + \frac{r}{2}\right)\left(U + \frac{R}{2} + \frac{r}{2}\right).$$

Using our parametrization for $a$ and $d$ given in equations (7.4) and (7.6) respectively, we can write down the factorization for $g$ over $k[r, R]$:

$$g(X) = f_6 \prod_{i=1}^{6} (X - w_i) \tag{B.1}$$

where

$$f_6 = \left(\frac{1}{-\operatorname{disc}(f)\cdot f(s)}\right)^3 = \frac{1}{\left(4b^3 + 27c^2\right)^3\left(s^3 + bs + c\right)^3}$$

and:

$$\begin{aligned}
w_1 &= \frac{1}{2}\Big(\left(-3s^2 - b\right)r^2 + (-4bs - 6c)\,r - bs^2 - 6cs + b^2\Big)R \\
w_2 &= \frac{1}{2}\Big(\left(3s^2 + b\right)r^2 + (4bs + 6c)\,r + bs^2 + 6cs - b^2\Big)R \\
w_3 &= \frac{1}{2}\Big(\left(-3s^2 - b\right)r^2 + (2bs + 3c)\,r - bs^2 + 3cs - b^2\Big)R \\
&\quad + \frac{1}{2}\Big((-3bs - 9c)\,r^2 + \left(9cs - 2b^2\right)r - 4b^2s - 6bc\Big) \\
w_4 &= \frac{1}{2}\Big(\left(3s^2 + b\right)r^2 + (-2bs - 3c)\,r + bs^2 - 3cs + b^2\Big)R \\
&\quad + \frac{1}{2}\Big((3bs + 9c)\,r^2 + \left(-9cs + 2b^2\right)r + 4b^2s + 6bc\Big) \\
w_5 &= \frac{1}{2}\Big(\left(-3s^2 - b\right)r^2 + (2bs + 3c)\,r - bs^2 + 3cs - b^2\Big)R \\
&\quad + \frac{1}{2}\Big((3bs + 9c)\,r^2 + \left(-9cs + 2b^2\right)r + 4b^2s + 6bc\Big) \\
w_6 &= \frac{1}{2}\Big(\left(3s^2 + b\right)r^2 + (-2bs - 3c)\,r + bs^2 - 3cs + b^2\Big)R \\
&\quad + \frac{1}{2}\Big((-3bs - 9c)\,r^2 + \left(9cs - 2b^2\right)r - 4b^2s - 6bc\Big)
\end{aligned}$$

## Appendix C. A representation for a $(4,4)$-split genus 2 curve

Let $E_1$ be an elliptic curve over $k$ given by $V^2 = U^3 + bU + c$ for scalars $b$ and $c$ and let $C_4$ be a genus 2 curve which is a degree 4 cover of $E_1$. Then there exists a scalar $s$ such that a representation for $C_4$ is given by $Y^2 = F(X)$ where:

$$
\begin{aligned}
F(X) = {} & \frac{(s^3+bs+c)\left(27cs^3-18b^2s^2-27bcs-2b^3-27c^2\right)}{\left(4b^3+27c^2\right)^3\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X^6 \\
& + \frac{3\left(s^3+bs+c\right)^2\left(3s^2+b\right)}{\left(4b^3+27c^2\right)^2\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X^5 \\
& + \frac{3\left(s^3+bs+c\right)E}{4\left(4b^3+27c^2\right)^2\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X^4 \\
& + \frac{-\left(s^3+bs+c\right)^2G}{2\left(4b^3+27c^2\right)\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X^3 \\
& + \frac{-\left(s^3+bs+c\right)H}{16\left(4b^3+27c^2\right)\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X^2 \\
& + \frac{3\left(s^3+bs+c\right)^2\left(3s^4+6bs^2+12cs-b^2\right)J}{16\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X \\
& + \frac{-\left(s^3+bs+c\right)JK}{64\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}
\end{aligned}
\tag{C.1}
$$

and where

$$
\begin{aligned}
E &= 9cs^7-26b^2s^6-171bcs^5+34b^3s^4-333c^2s^4+155b^2cs^3-6b^4s^2+126bc^2s^2 \\
&\quad +7b^3cs+144c^3s-2b^5-17b^2c^2 \\
G &= 7s^6+23bs^4+68cs^3-11b^2s^2-4bcs-3b^3-20c^2 \\
H &= 27cs^{11}+6b^2s^{10}+585bcs^9-402b^3s^8+2349c^2s^8-3330b^2cs^7+460b^4s^6 \\
&\quad -6156bc^2s^6+1410b^3cs^5-7776c^3s^5+140b^5s^4+4230b^2c^2s^4+23b^4cs^3 \\
&\quad +3024bc^3s^3+46b^6s^2+516b^3c^2s^2+3024c^4s^2+5b^5cs-48b^2c^3s+6b^7 \\
&\quad +85b^4c^2+288bc^4 \\
J &= s^6+5bs^4+20cs^3-5b^2s^2-4bcs-b^3-8c^2 \\
K &= 27cs^9-54b^2s^8-324bcs^7+36b^3s^6-891c^2s^6+378b^2cs^5-72b^4s^4 \\
&\quad +81bc^2s^4-36b^3cs^3+324c^3s^3-36b^5s^2-297b^2c^2s^2-45b^4cs-324bc^3s \\
&\quad -2b^6-45b^3c^2-216c^4
\end{aligned}
$$

## References


1. Oskar Bolza, *Ueber die reduction hyperelliptischer integrale erster ordnung und erster gattung auf elliptische durch eine transformation vierten grade*, Math. Ann. **28** (1887), no. 3, 447–456.
2. Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)
3. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR1484478
4. Jean-Benoît Bost and Jean-François Mestre, *Moyenne arithmético-géométrique et périodes des courbes de genre* 1 *et* 2, Gaz. Math. (1988), no. 38, 36–64. MR970659 (89k:14072)

5. Nils Bruin, *Visualising Sha[2] in abelian surfaces*, Math. Comp. **73** (2004), no. 247, 1459–1476 (electronic). MR2047096 (2005c:11067)
6. Nils Bruin and Kevin Doerksen, *Electronic resources*, `http://www.cecm.sfu.ca/~nbruin/splitigusa`.
7. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR1406090 (97i:11071)
8. Ron Donagi and Ron Livné, *The arithmetic-geometric mean and isogenies for curves of higher genus*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28** (1999), no. 2, 323–339. MR1736231 (2001a:14022)
9. Gerhard Frey and Ernst Kani, *Curves of genus* 2 *covering elliptic curves and an arithmetical application*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 153–176. MR1085258 (91k:14014)
10. P. Gaudry and É. Schost, *On the invariants of the quotients of the Jacobian of a curve of genus 2*, Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001), Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 373–386. MR1913484 (2003e:14020)
11. Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR0114819 (22 #5637)
12. ———, *On Siegel modular forms of genus two*, Amer. J. Math. **84** (1962), 175–200. MR0141643 (25 #5040)
13. Ernst Kani, *Elliptic curves on abelian surfaces*, Manuscripta Math. **84** (1994), no. 2, 199–223. MR1285957 (95i:14042)
14. Luise-Charlotte Kappe and Bette Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly **96** (1989), no. 2, 133–137. MR992075 (90i:12006)
15. A. Krazer, *Lehrbuch der thetafunktionen*, Teubner, Leipzig, 1903.
16. Robert M. Kuhn, *Curves of genus* 2 *with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988), no. 1, 41–49. MR936803 (89f:14027)
17. Herbert Lange, *Über die Modulvarietät der Kurven vom Geschlecht* 2, J. Reine Angew. Math. **281** (1976), 80–96. MR0407029 (53 #10812)
18. K. Magaard, T. Shaska, H. Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Preprint 2-2008, Inst. Exp. Math., Essen.
19. J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR861974
20. Naoki Murabayashi, *The moduli space of curves of genus two covering elliptic curves*, Manuscripta Math. **84** (1994), no. 2, 125–133. MR1285952 (95f:14046)
21. T. Shaska, *Curves of genus 2 with* $(N,N)$ *decomposable Jacobians*, J. Symbolic Comput. **31** (2001), no. 5, 603–617. MR1828706 (2002m:14023)
22. ———, *Genus 2 curves with* $(3,3)$*-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 205–218. MR2041085 (2005e:14048)
23. ———, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR2039100 (2004m:11097)
24. Alice Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 447–461. MR1638488
25. Benjamin Smith, *Explicit endomorphisms and correspondences*, Ph.D. thesis, University of Sydney, 2005 `http://hdl.handle.net/2123/1066`.

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6
*E-mail address*: `nbruin@sfu.ca`

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6
*E-mail address*: `kdoerkse@sfu.ca`